

SISTEMA DE CONTROLE DE CONTRATOS INTELIGENTES

Ricardo de Souza Martins¹ <xrsmartins@hotmail.com>
Elgio Schlemer² <elgio.schlemer@ulbra.br> – Orientador

Universidade Luterana do Brasil (Ulbra) – Curso de Ciência da Computação – Câmpus Gravataí
Av. Itacolomi, 3.600 – Bairro São Vicente – CEP 94170-240 – Gravataí - RS

26 de novembro de 2018

RESUMO

Este artigo tem por objetivo explorar a origem e natureza das moedas digitais bem como a sua criação, e por conseguinte, as características da blockchain e suas aplicações. Também deve explorar o seu propósito e suas influências no mundo digital assim como a sua viabilidade como instrumento de contratos digitais e o entrelaçamento de suas relações econômicas dentro da era pós-moderna.

Palavras-chave: Blockchain, Moedas digitais, Economia, Contratos inteligentes

ABSTRACT

Title: “Smart contracts control system”

This article aims to explore the origin and nature of digital coins as well as their creation and therefore the characteristics of the blockchain and its applications. It must also explore its purpose and its influences in the digital world, as well as its viability as an instrument of digital contracts and the interweaving of its economic relations within the postmodern era.

Key-words Blockchain, Digital currencies, Economy, Smart contracts

1 INTRODUÇÃO

Partindo do princípio de que neste começo de século XXI herdou-se do anterior algumas importantes conjecturas, entre elas a Internet com a qual torna-se possível interligar extremos do planeta, fazendo o conhecimento se multiplicar de forma vertical e veloz, trazendo consigo uma vasta gama de novidades.

Uma delas no qual muitos se debruçam e tem atraído muitos interesses, por se tratar de algo novo que quebra alguns paradigmas que até então pareciam inquebráveis, é o Bitcoin. Com uma proposta revolucionária e inovadora em seu fundamento, nem tanto por ser mais uma moeda, mas pelo fato de como ela é gerada e de como é sustentada, rompendo com a maioria das relações de valores contemporâneos até então estabelecidos.

Outro importante movimento inovador que se apresenta nos tempos pós-modernos e nasce junto com a inovação tecnológica, que apresenta riscos incompatíveis para o mercado de capital convencional, é o *Crowdfunding*.

Trata-se de financiamento de um projeto por um grupo independente de indivíduos, realizado por meio da Internet sem intermediários profissionais (Schwienbacher & Larralde, 2012) e que proporciona o rompimento da aplicação do investimento na forma tradicional e beneficia a natalidade de empresas inovadoras de tecnologia que surgem em padrões acelerados e portanto conflitantes com o mercado de capital atual.

Neste contexto o tema deste trabalho procura explorar os aspectos econômicos e as relações comerciais que o fenômeno Bitcoin causa no mundo financeiro e econômico e sua relação com os

¹ Aluno da disciplina de Trabalho de Conclusão de Curso do Bacharelado em Ciência da Computação na Ulbra Gravataí.

² Professor das disciplinas da área de Sistemas Operacionais dos cursos de Ciência da Computação e Sistemas de Informação, na Ulbra Canoas e Ulbra Gravataí. Coordenador das disciplinas de Trabalho de Conclusão de Curso do Bacharelado em Ciência da Computação na Ulbra Gravataí.

movimentos oriundos dos novos paradigmas que procuram se estabelecer e principalmente o seu uso como forma efetiva de participação no sistema financeiro mundial e o estreitamento de sua relação contextual na sociedade.

Para isso será explorada a relação das moedas digitais na economia, suas novas ferramentas e tecnologias oriundas do comércio digital e como estas se relacionam..

Explorar-se-á uma das relações de comércio que é o centro das atividades comerciais, o contrato que sem dúvida faz parte do cotidiano das relações sociais e principalmente das relações econômicas.

Com um conceito bem objetivo Beviláqua (1950) diz que o contrato é: “o acordo de vontade entre duas ou mais pessoas com a finalidade de adquirir, resguardar, modificar ou extinguir direitos”, sempre no intuito de gerar harmonia entre as relações humanas e que também evolui com estas relações e tende a aprimorar-se junto com os novos tempos. E com o advento das moedas digitais não seria difícil de imaginar que os contratos também venham a aparecer em suas versões de formato digital.

Devido ao fato de que as moedas virtuais vem tomando um grande número de seguidores e de que elas ainda não são compreendidas, de uma forma geral, sem que haja um conhecimento mais aprofundado no assunto faz-se necessário o aprimoramento de ferramentas que possibilitem a melhoria da interação das mesmas e que facilitem não só a sua compreensão mas principalmente o seu uso de forma mais abrangente.

Apesar de ter muitos entusiastas, principalmente no meio acadêmico e econômico, ainda há uma grande lacuna a ser preenchida no que diz respeito a usabilidade, por estar muito preso ao conhecimento específico. Por isso existe a necessidade da criação de aplicações que estejam mais voltada ao público leigo e que procure diminuir as distâncias do mundo técnico com o mundo do cotidiano.

De acordo com Howkins (2001), a criatividade não é monopólio dos artistas ou de alguma ciência, mas está presente nos empresários, economistas, cientistas, ou seja, está nas pessoas, pois eles têm a capacidade de criar algo novo, original, pessoal, significativo e real.

Sendo assim, tanto o aparecimento de novos conceitos quanto as novas ferramentas, já disponíveis, que se apresentam nos tempos atuais, carregam em si um sentimento e uma percepção de que algo novo está sempre prestes a aparecer.

2 INTERNET E A ECONOMIA

Uma boa definição de Internet é encontrada no livro de CASTELLS (2003, p.7): “A tecnologia da informação é hoje o que a eletricidade foi para a Era Industrial”, ou seja, algo indispensável e que tem a capacidade, assim como um motor, de distribuir a informação com uma força bem expressiva. Ela é, na verdade, uma rede de força computacional e potencialmente voltada a transmissão da informação em tempo real.

A Internet nasceu nos tempos da guerra fria, criada pelo governo dos EUA no final dos anos 70. Foi criada pela agência do Departamento de Defesa denominado ARPA (*Advanced Research Projects Agency*), que criou um programa chamado Arpanet, com a finalidade de facilitar o fluxo de pesquisa e o compartilhamento on-line de tempo de computação.

Com o auxílio de algumas universidades americanas e do surgimento de algumas novas técnicas de rede, como a criação do protocolo TCP/IP, desenvolvido na Universidade Da Califórnia do Sul, em 1975 foi se expandindo para o uso de todas as forças armadas do país.

Por questões de segurança, em 1984 os EUA criou uma rede independente para uso exclusivo militar, a MILNET, sendo assim, a Arpanet tornou-se a ARPA-Internet para fins de pesquisas gerais. Finalmente em 1990 a Internet foi privatizada e como a maioria dos computadores desde 1980 já

possuíam a tecnologia de rede, teve-se o crescimento da rede até chegarmos nas dimensões que hoje conhecemos.

Mais recentemente apareceu um novo conceito que é o IoT (*Internet Of Things* - Internet das coisas), um termo genérico que teve sua primeira citação em 1999 por *Kevin Ashton* (ASHTON 2009) e que tomou fôlego na última década, e que basicamente expressa a presença da internet em um conceito bem mais amplo do que o inicial levando ela para dentro das coisas. Ex: Tvs, Telefones, Rádios, Relógios, etc... e fazendo que as coisas interagem diretamente na rede com seus próprios meios de coleta de informação através de seus sensores, câmeras, etc... Enraizando cada vez mais os conceitos digitais.

2.1 Economia digital

Com a advento da Internet e sua globalização, surge uma economia inerente a este fato, que traz consigo novas perspectivas junto às novas tecnologias e aos novos paradigmas. Neste contexto surge um novo mercado e apresenta um leque de possibilidades para o comércio e serviço agregando também os novos desafios.

No começo do século XXI a economia, oriunda das governanças e do capitalismo baseada no monopólio da emissão de moedas controlados por bancos centrais, apresenta uma crise de proporções globais, levadas segundo Ulrich (2014) pela desregulamentação do setor, a ganância, o excesso dos bancos ou simplesmente o capitalismo na sua essência tendo o seu ápice com a quebra do banco Lehman Brothers, em setembro de 2008, e que é a maior falência dos Estados Unidos até então. Este fato contribuiu para que as cogitações de criação de ativos alternativos viessem a ser pesquisados com mais força.

Por ser adaptável a quase todos os setores da economia pré-existente, o mercado digital tem um crescimento notável nos últimos dez anos e à medida que a Internet se desenvolve o comércio digital acompanha de perto este movimento.

Este espaço é atrativo a pequenas e médias empresas que têm margens apertadas e tentam explorar este universo de baixo custo e grandes perspectivas e dando a estes um fôlego novo.

Além disso o surgimento das Empresas de base tecnológicas (EBTs), que trazem conhecimento tecnológico científico, empregando técnicas pioneiras e avançadas na obtenção de produtos e serviços (Meirelles et al., 2008) agregam enormes valores a este mercado em plena expansão.

2.2 Moeda digital

O modo de relação dos valores através da história nos mostra que a moeda é algo bem antigo e traz em si mesmo o esforço do homem em facilitar o cotidiano da vida. Galbraith (1997, p.5) diz que “a moeda é um artigo de conveniência bastante antigo, mas a noção de que é um artefato seguro, aceito sem discussão, é em todos os sentidos, um fato bastante ocasional”. Ele nos revela o quanto uma moeda é ocasional, desde os primórdios tempos quando o Ouro ou a Prata eram moedas de troca, assim como bens e serviços já serviram para este fim.

Trocada diversas vezes através dos tempos, como o Brasil fez abandonando o Cruzeiro e aderindo ao Real, a moeda tem se aperfeiçoado, mudando com o passar da história, caminhando junto com a humanidade e seus desafios.

Muitos avanços na criação e gerenciamento da moeda acompanham os avanços tecnológicos, como o advento de instituições financeiras que criaram outras formas de representar a moeda como o cheque e o cartão de crédito. Com todo este contexto é que, no dia 11 de fevereiro de 2009 foi publicado do grupo P2P Foundation por Nakamoto (2009) um conceito do que pode-se chamar de moeda pós-moderna, o Bitcoin. Sendo esta a tentativa mais bem sucedida de criação de uma moeda totalmente digital até então implementada.

2.3 Bitcoin

O Bitcoin nasceu em meio mais uma grande crise financeira para oferecer uma alternativa de rompimento com a moeda centralizada e operada por governos que desde o começo do século XX, principalmente após a 1ª guerra mundial, começaram a emitir moedas para fabricar receitas e assim monopolizar o poder através da economia.

Diferente do que não acontecia na antiguidade onde as *Commodities*³, geralmente ouro ou prata, faziam o papel universal da moeda e servia bem ao mundo pelo seu caráter livre, sem fronteiras, a centralização trouxe muitos problemas.

Então, como um meio de libertação deste sistema de capital centralizado e dominado por governos e suas moedas, o Bitcoin se apresenta, não só como mais uma moeda, mas tenta resgatar os valores que outrora existiam e ainda acrescenta a estes outros valores novos para fazer frente às crises que este sistema centralizado sofre.

Uma boa definição do que é Bitcoin:

Bitcoin é um conjunto de conceitos e tecnologias que formam a base de um ecossistema de dinheiro digital. As unidades de moeda chamadas bitcoins são usadas para armazenar e transmitir valor entre os participantes na rede Bitcoin Antonopoulos(2016)

Segundo Ulrich (2014) “o Bitcoin é a maior inovação tecnológica desde a Internet, é revolucionário, sem precedentes e tem o potencial de mudar o mundo de uma forma jamais vista”, com esta empolgada definição entramos na parte mais “revolucionária” do bitcoin, que é a sua rede chamada de Blockchain, pois o protocolo deste de nada valeria sem o daquele, porque um não existe sem o outro e os dois formam a solução descentralizada completa.

Seu criador permanece anônimo autodenominado de Satoshi Nakamoto. Ele permanece assim apesar de todas as tentativas frustradas de o encontrarem e seus Bitcoins permanecem intocados até então.

2.4 A Blockchain

Trata-se de uma rede que usa a tecnologia P2P e permite que o protocolo se propague e possibilite a transferência da moeda entre seus membros onde qualquer pessoa, que quiser, pode participar por tratar-se de um software de código aberto, podendo ser executado de vários dispositivos como: computadores pessoais, notebooks e smartphones, pois ela é uma tecnologia que tem amplo acesso.

Entre suas propriedades está a de ser um enorme livro contábil, público no qual se encontra registrado todas as transações de Bitcoin assim como todas as moedas que entraram em circulação durante toda a sua existência, além de toda esta transparência, ela ainda permite que uma pessoa passe suas moedas para outra sem a interferência de um intermediário como um Banco por exemplo, por se tratar de um Peer to Peer (Ponto a Ponto), onde cada ponto verifica a veracidade das informações e transações ocorridas.

Na figura 1 tem-se um idéia de como funciona a blockchain, como uma teia de computadores interligados formando uma corrente de blocos interligados, cada ponto tem uma cópia fiel da corrente

³ *Commodity*, em economia ,é tudo aquilo que, se apresenta em seu estado bruto (mineral, vegetal etc), pode ser produzido em larga escala e agrega valor.

inteira.

Figura 1 - Blockchain



Fonte: <https://portaldobitcoin.com>

2.5 A segurança Bitcoin

A segurança é um ponto crucial para a vida de qualquer moeda, e se tratando de Internet mais ainda. O incrível é que o Bitcoin também revoluciona neste aspecto, porque implantou algo novo até então, a *Proof of work* (Prova de Trabalho).

Usando criptografia avançada e encadeada na corrente de blocos (blockchain), a prova de trabalho resolveu um dos maiores problemas da computação distribuída sem a intervenção de terceiros, firmando os blocos com segurança na cadeia P2P.

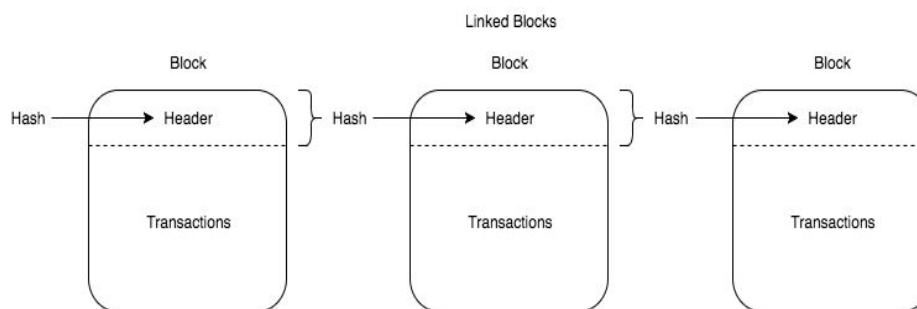
A *Proof of work*, um dos pontos fortes do protocolo Bitcoin, garante a veracidade da informação usando o consenso da rede, através do poder computacional dos próprios clientes, que ainda podem receber recompensas por seu trabalho da própria rede.

Com seus blocos encadeados, um por um pelos hashes⁴ em toda a cadeia da blockchain desde o primeiro bloco, denominado bloco gênese, até o último não pode sofrer alteração em nada, porque qualquer alteração levaria a mudança de todos os blocos subsequentes gerando uma desconformidade com a rede e fazendo com que este bloco fosse retirado da mesma, fazendo com que este fato traga uma segurança ímpar para toda a rede e trazendo sustentação ao protocolo bitcoin.

A figura 2 mostra o encadeamento dos blocos onde os hashes de cada bloco, que foram calculados pela prova de trabalho, junto com o hash do bloco anterior, e criaram um número matemático único em cima de uma cadeia de caracteres, são entrelaçados formando uma corrente contínua e uniforme, onde suas transações de Bitcoin podem se estabelecer de um modo transparente para toda a rede.

⁴ Hash: Sequência de números geradas por um algoritmo computacional

Figura 2 - hash da blockchain



Fonte: <https://www.pluralsight.com/guides/blockchain-architecture>

2.6 CROWDFUNDING

No começo do século XX com as guerras mundiais expandindo o processo produtivo capitalista e o surgimento das grandes empresas multinacionais tomando a atenção do mercado, a economia acabou afastando-se das pequenas e médias empresas. Para manter o poder do capital, os países centralizaram a economia nos bancos.

Segundo Corrêa (2016) muitas empresas emergentes têm dificuldades de conseguir financiamentos por não terem histórico de créditos e não terem garantias suficientes para calçar as dívidas, impossibilitando que as mesmas pudessem investir e principalmente às empresas emergentes de tecnologia, conhecidas como *startups*⁵, que encontraram ainda mais dificuldades em conseguir financiamentos pois apresentam um risco grande para o atual e burocrático sistema financeiro, o que incentivou a essas empresas a busca de novos horizontes.

Com o avanço da tecnologia e o crescimento do mercado digital fez-se necessário o aparelhamento de novas soluções, onde o *crowdfunding* se encaixa, principalmente por ser oriundo da mesma fonte, a Internet.

Corrêa (2016) relata que em 1997 uma banda de rock inglesa chamada “Marillion” conseguiu de seus fãs, através de doações pela Internet, a quantia de £39.000,00 (trinta e nove mil libras esterlinas) para a realização de uma turnê nos EUA. Este relato mostra o potencial que a Internet tem a oferecer na captação de recursos e como o *crowdfunding* se mostra uma ferramenta eficiente na captação de recursos, sendo uma alternativa viável de financiamento.

Na figura 3 tem-se uma visão simples do conceito, onde a caixa pode representar uma conta bancária ou uma carteira de bitcoins, por exemplo, e centraliza a arrecadação dos recursos, possibilitando a fácil e ágil manutenção dos mesmos.

⁵ Startup: Empresas emergentes de tecnologia

Figura 3 - Crowdfunding



Fonte: <https://neritpolitica.com.br/blog/crowdfunding-para-campanha-eleitoral>

Segundo Ponteza e Oliveira(2016) o *crowdfunding* é uma forma de recolher recursos que utiliza a força e a mobilização das massas (a crowd), geralmente pela Internet, com o objetivo de agilizar o processo da captação dos recursos e a diminuição de custos e burocracia.

As startups não demoraram para usufruírem desta ferramenta e colaborarem para que o *crowdfunding* fosse explorado e se tornasse uma boa alternativa para seus problemas de captação de recursos para investimentos

Em virtude desta ferramenta ser uma alternativa frente a economia tradicional, liberta de paradigmas outrora impostos pelo sistema financeiro, e principalmente de sua governança, tendo em vista as já existentes moedas virtuais e principalmente o Bitcoin, sendo oriundo do mesmo ecossistema, não é difícil imaginar que elas possam trabalharem juntas, estreitando as relações, dentro da economia digital.

3 CONTRATOS INTELIGENTE

Seja aplicado por um governo ou de qualquer outra forma, o contrato é o alicerce básico de uma economia de mercado, nas relações de comércio, bens e serviços, fazem parte da história da evolução da sociedade.

Diante das mais diversas teorias, uma em especial tem tomado fôlego com o advento da Blockchain, os chamados contratos inteligentes (*smart contracts*), conceito proposto por Szabo (1996), no qual é proposto que traduza-se as cláusulas de um contrato para um software que pudesse ser auto-executáveis com o objetivo de diminuir a interferência de terceiros para a manutenção do mesmo.

A partir da Blockchain, como uma rede estável e segura surge então a renovação do *Smart Contract*, assim se torna possível criar uma Máquina Virtual⁶ distribuída capaz de executar scripts sob a tutela da rede, que se encarrega de pôr os softwares em execução e ainda fazer qualquer transferência de valores geradas por estes .

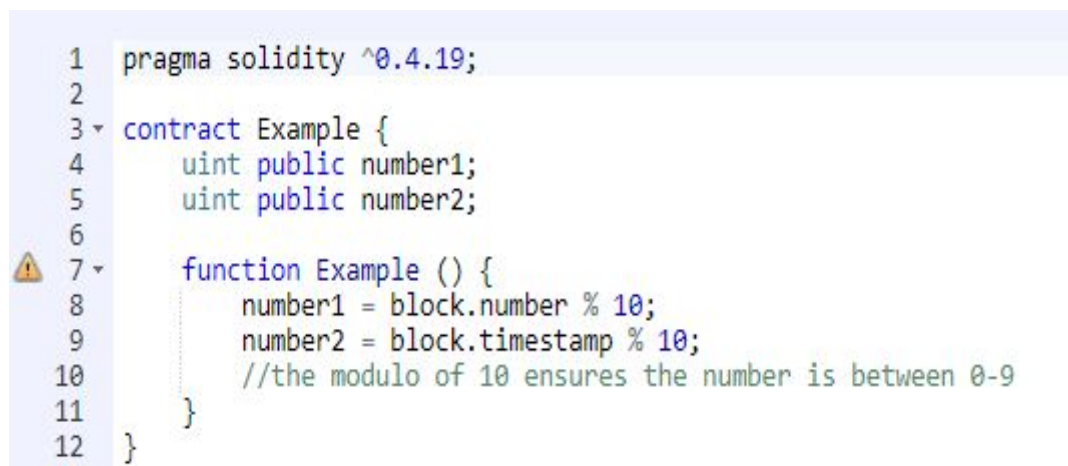
Uma das pioneiras na implantação de Blockchain com contratos inteligentes é o *Ethereum* de

⁶ (Virtual Machine) Software que simula o ambiente computacional, que executa programas como um computador real

BUTERIN(2013), criado com a intenção de ser um protocolo alternativo para a criação de aplicações descentralizadas, totalmente baseada, na sua essência, no *Bitcoin*, porém implementando o conceito proposto por Szabo (1996). O *Ethereum* tornou-se a segunda criptomoeda de maior capitalização até o momento, proporcionando a criação das ICOs⁷.

Na figura 4 ve-se um exemplo de um contrato inteligente escrito na linguagem de programação Solidity versão 0.4.19. Nota-se que o programa direcionado a objetos reconhece uma palavra reservada chama Contract (Contrato em português), onde engloba toda a programação do contrato inteligente.

Figura 4 - Solidity



```
1  pragma solidity ^0.4.19;
2
3  contract Example {
4      uint public number1;
5      uint public number2;
6
7      function Example () {
8          number1 = block.number % 10;
9          number2 = block.timestamp % 10;
10         //the modulo of 10 ensures the number is between 0-9
11     }
12 }
```

Fonte:

<https://medium.com/@agosh.saini/gambling-using-smart-contract-why-is-it-difficult-88079cbb86de>

Sempre atenta aos novos conceitos as *Startups*, com o intuito de resolver seus problemas de financiamentos junto às novas tecnologias, aplicaram os primeiros *crowdfunding* de criptomoedas. Baseadas em contratos inteligentes, elas foram denominadas ICOs e são responsáveis pela multiplicação de criptomoedas e tendem a aperfeiçoar as relações de contrato e moeda e já oferecem oportunidades de negócios mais confiáveis neste meio inovador e complexo.

4 PROPOSTA DE TRABALHO

Com o intuito de aplicar as novas tecnologias oriundas da *Blockchain* será feito uso do *Smart Contract* (Contrato Inteligente) em uma plataforma web, para a criação e controle destes contratos. Levando em conta alguns conceitos das moedas digitais, principalmente do Bitcoin e expandindo-os como ferramentas nesta aplicação.

Explorar-se-á algumas tecnologias bem recentes, como a linguagem de programação *Solidity* que funciona em ambientes distribuídos, e a sua interação automatizada com as criptomoedas, usando também conceitos de programação web como o MVC⁸ para o controle e manipulação dos dados de forma ordenada e dando prioridades para softwares open-sources.

A plataforma também tem por objetivo, além de poder gerar os contratos, apresentá-los de uma forma amigável, de fácil acesso e compreensão, possibilitando a interação com os mesmos de forma completa

Deverá ser aplicado alguns conceitos de segurança principalmente referente a banco de dados, com o uso de algumas técnicas como hash e salt-number e também o uso de APIs, como o Google Authenticator, para o login na plataforma.

⁷ ICO: *Initial Coin Offering (Oferta inicial da moeda)*.

⁸ MVC (Model View Controller): é um padrão de arquitetura de software

4.1 TECNOLOGIAS APLICADAS

Para o desenvolvimento do projeto web para a interação e concepção de contratos inteligentes far-se-á uso de algumas ferramentas que serão adotadas para implementação da aplicação, no qual se abordará as principais tecnologias e suas características mais importantes:

- **Apache:** Criado em 1995 por Rob McCool, é o servidor HTTP de código livre muito popular e um dos mais bem sucedidos que existe nesta área, geralmente implantado em plataforma linux, servirá de base para a aplicação web.
- **Python:** Linguagem de Programação criada por Guido van Rossum em 1991, bem objetiva moderna, multi paradigma, orientada a objeto e com amplo amadurecimento de suas bibliotecas segundo Milmann e Avaizis(2011)., tem se destacado muito nos últimos anos nas indústrias e na computação científica.
- **Django:** Framework escrito com base na linguagem Python e direcionado para web, trabalha na camada do servidor, permitindo que a programação python tenha um canal direcionado para a web.
- **Virtualenv:** Ferramenta para criação de ambientes python independentes, que isolam, de forma automática configurações, plugins e bibliotecas.
- **Nodejs:** Desenvolvido em 2009 por Ryan Dahl, Node.js (ou apenas Node) é um ambiente JavaScript single-threaded do lado do servidor implementado em C e C ++, no qual oferece um desempenho ágil, útil e funcional.
- **Solidity:** Linguagem de programação de alto nível, desenvolvida originalmente por Gavin Wood em 2014,e que foi resgatada pela equipe da Ethereum para a confecção dos contratos inteligentes, amplamente utilizada por várias plataformas, com interação completa em uma *Blockchain*.
- **MariaDB:** Banco de dados relacional criado pelos desenvolvedores do Mysql que após a sua aquisição em 2009 pela Oracle Corporation, uma empresa privada, as equipes de criação do Mysql saíram e fundaram o MariaDB Foundation, de código aberto, é altamente compatível com o Mysql.

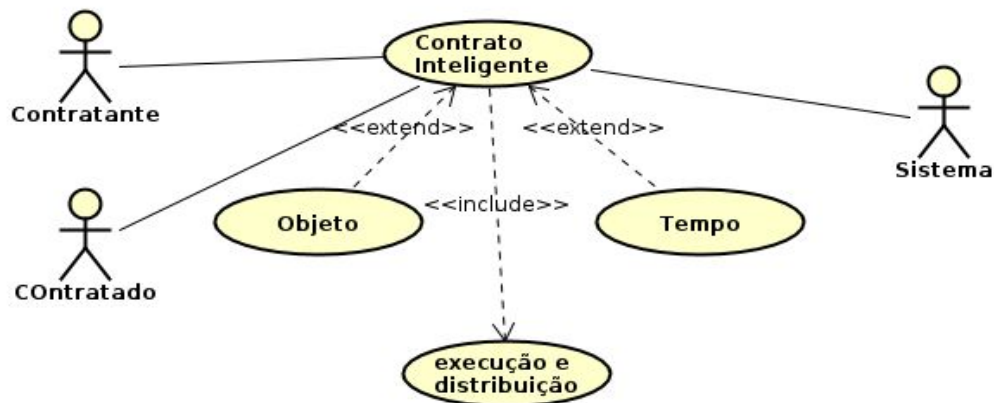
Procurou-se prioritariamente o uso de ferramentas de desenvolvimento de código aberto, de comunidade ativa e de reconhecida reputação.

4.2 MODELAGEM

Para o caso de uso da aplicação será implementado um sistema de criação e controle de contratos inteligentes via web com pagamento em moeda virtual. No caso o contrato inteligente vai ser o agente distribuidor dos recursos de forma automática dentro de um cronograma em linha de tempo ou por consenso, com possibilidade de interação mútua entre as partes integrantes do contrato.

A figura 5 mostra um caso de uso da aplicação inerente ao contrato inteligente que se relaciona com o sistema e com as partes integrantes que de modo geral participam com as informações e deixam para o contrato as ações principais da execução do mesmo e distribuição, seja de ativos ou de informações referentes a sua execução.

Figura 5 - Diagrama de caso de uso



Ao mesmo tempo em que os contratos são executados a aplicação organiza e guarda as informações, monitorando todas as transações do mesmo em paralelo.

Para que o contrato possa ser gerido pela aplicação é necessário que ambas as partes, contratado e contratante, assinem o mesmo com uma criptografia assimétrica e as suas chaves públicas e privadas.

As assinaturas garantem a mutualidade das informações do contrato suas regras e suas diretrizes, bem como, da concordância de todas as partes representadas pelo contrato, que uma vez implementado não poderá ser alterado, até que cumpra todo seu propósito.

Será necessário a criação de banco de dados para o armazenamento dos dados de login do usuário, dos clientes (contratados ou contratantes) e dos contratos com seus objetos e descrições.

O sistema terá dois tipos de acesso que é o nível admin e o nível usuário, onde o admin poderá ter total e completo acesso a todas as funcionalidades da aplicação e o usuário com parcial acesso.

4.3 IMPLEMENTAÇÃO

Para o desenvolvimento da aplicação web será necessário a configuração de um servidor com sistema operacional *Linux*, com serviço de HTTP *Apache*. Será necessário a instalação do Nodejs para a interação com o HTTP e também para a implantação do compilador para a linguagem *Solidity*.

Por haver a necessidade de implantação de um nó blockchain para o acompanhamento do contrato e sua perfeita integração com o sistema web, algumas bibliotecas serão usadas.

Para o uso dos *smart contracts* tem-se como referência o Ethereum, desenvolvido por Buterin (2013), que acrescentou em sua plataforma blockchain a implementação de vários serviços entre eles o Web3, também conhecida como web 3.0, e que é o SDK⁹ principal para interação com a plataforma, baseada em Javascript, mas que também é oferecida em outras linguagens de programação como *Python* e *C++*.

O Geth é uma das alternativa para a implementação de um nó¹⁰ ethereum que será usado para espelhar a blockchain em nosso servidor e interagir com o universo dos contatos e moedas virtuais web3, nos dando a possibilidade de implantação de carteiras, transferências de valores e claro a implementação e interação com os contratos inteligentes.

O Solidity é uma linguagem de programação em alto nível orientada a objeto baseada em

⁹ SDK:(Software Development Kit) kit de desenvolvimento de software

¹⁰ Nó: trata-se de uma cópia fiel da blockchain

C++, Python e principalmente em Javascript, sua criação foi direcionada para o desenvolvimento dos *smart contracts* e funciona sob a Ethereum Virtual Machine (EVM) dentro da *blockchain* do Ethereum.

Um banco de dados é necessário para a guarda das informações dos usuários, dos contratos e manutenção do sistema onde deverá ser usado um SGBD (Sistema de Gerenciamento de Banco de Dados) denominado MariaDB.

Para a interface web será usado um framework Python chamado *Django*, com uma ferramenta que isola aplicações em Python chamado Virtualenv, o que permitirá o compartilhamento do servidor Apache com as configurações da Blockchain do Ethereum em conjunto com as tecnologias de interface web.

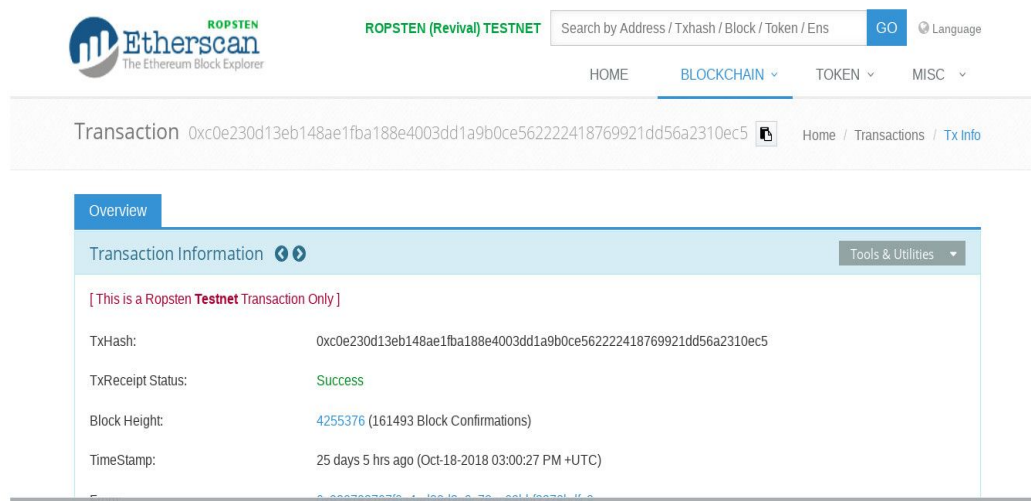
4.4 TESTES PRELIMINARES

Após as instalações do Geth se faz necessário a aplicação de uma Blockchain local para testes preliminares onde são testadas a comunicação das aplicações principalmente com o compilador Solidity de onde vai ser abstraído o código nativo que deverá ser interpretado pelo EVM na Blockchain.

Com esta ação local sendo o primeiro passo, tendo a blockchain já em funcionamento, deverá ser efetuados os testes com o compilador e seus códigos rodando dentro da blockchain local; depois de tudo ajustado o próximo passo é usar uma Blockchain de testes.

Existe várias blockchains paralelas a original que são chamadas de Testnet e são geralmente fornecidas pelo desenvolvedor que provavelmente executaram seus testes antes de seus lançamento oficiais e disponibilizaram para as comunidades de programadores em geral. A figura 6 apresenta o site da Ropsten que fornece acesso a uma destas Blockchain de teste.

Figura 6 - Ropsten



Fonte: <https://ropsten.etherscan.io/>

4.5 TESTES AVANÇADOS

Na sequência, com todas as ferramentas configuradas e testadas, o próximo passo é sincronizar a blockchain com a do Ropsten, para isso basta configurar o geth para direcionar a sincronização da Blockchain local com a blockchain do Testnet. Após essa sincronização será possível jogar os contratos feitos pelo servidor na rede P2P e acompanhar o seu desdobramento.

Os testes destes contratos já se farão em tempo real com a rede global e poderá ser

acompanhada pelo site da Ropsten, como demonstrada na figura 6, e todas as transações feitas nestes contratos serão simultâneos.

É importante ressaltar que a principal diferença da rede de teste e a rede oficial é a emissão de moedas, que no caso da rede de teste é livre, o que faz que a rede de testes não produza valores monetários, mas servindo com toda a tecnologia disponível até então para que as implementações tenham o máximo de êxito.

4.6 CRONOGRAMA

Descrição	Fevereiro				Março				Abril				Maio				junho			
	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Estudo de viabilidade técnica da proposta																				
Levantamento das ferramentas e custos																				
Implementação e configuração do servidor																				
Ajustes e testes no servidor																				
MN: capa, introdução																				
MN: Tecnologias aplicadas																				
MN: Concepção, modelagem, tecnologia																				
Implementação da blockchain no servidor																				
Modelagem do banco de dados																				
instalação do banco de dados																				
Preparação para o seminário de andamento																				
MN: Revisão e conclusão da monografia																				
Elaboração do pôster físico e virtual																				
MN: Testes e validações																				
MN: Ajustes relacionados a feedbacks do orientador																				
Apresentação da defesa junto à banca																				
Ajuste da monografia conforme à banca																				
MN = Monografia																				

5 CONSIDERAÇÕES FINAIS

Após o advento da *Internet*, algo que se tornou comum para as pessoas usufruírem, principalmente entre as mais jovens, como uma coisa banal e corriqueira mas que levou um certo tempo e a dedicação de muitos, que apostaram em um modo novo e eficaz de comunicação e relacionamento e que hoje podem se orgulhar de seus feitos.

Enquanto o tempo anda e a ciência se multiplica junto com o conhecimento, as possibilidades de acreditar que algo novo possa surgir a cada momento da história, principalmente em se tratando das ciências relacionadas à internet, onde tudo parece ser mais acelerado a cada minuto, se apresentam.

Viu-se neste artigo como foi o contexto da criação das moedas virtuais e como elas estão se interagindo com o mundo virtual e real, passando pela economia e sua interação com os novos conceitos estabelecidos até então.

Com a pesquisa feita neste trabalho mostrou-se viável a implementação de ferramentas que sirvam de apoio e facilitem a relação das moedas digitais com as pessoas em geral, principalmente dar acesso aos que por falta de um maior conhecimento técnico aprofundado não conseguem interagir com o mundo digital em sua ampla dimensão.

Assim tendo as moedas digitais como plano de fundo pode-se dar mais um passo a diante rumo ao futuro. Explorando a tecnologia de blockchain, que apresenta um leque de possibilidades viáveis para a criação de novas ferramentas capazes de interagir com esses novos conceitos, e ampliando os horizontes do conhecimento.

Fazendo-se uso dos Contratos Inteligentes (smart contracts), que parecem ser um fruto que está

prestes a amadurecer, muito mais que uma simples aposta, eles já possuem tecnologia que os assistam e à medida em que ela amadurece e sua viabilidade cresce também aumentam seus seguidores e já despertam a atenção de áreas como a do direito.

Apesar de se tratar de um assunto muito recente, o fruto deste estudo e a proposta deste trabalho mostram-se acessíveis e as tecnologias apresentadas plenamente viáveis, principalmente as que fundamentam as moedas virtuais.

Tendo como seu maior expoente os paradigmas originários do Bitcoin e seus desdobramentos no mundo virtual, já é possível vislumbrar o futuro com bons olhos, na expectativa de que em breve estaremos usufruindo de muitas boas ferramentas e que este trabalho seja apenas mais um em meio a multidão.

REFERÊNCIAS

ASHTON, Kevin. That ‘Internet of Things’ thing. Publicado no RFID Journal, 2009. Disponível em . Acesso em 03 Nov. 2018.

BUTERIN, Vitalik. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2013. URL {<http://ethereum.org/ethereum.html>}.

CORRÊA, M. M. (2016). Público alvo das ofertas públicas de títulos de dívida conversíveis em participação societária ofertados por meio de plataformas de equity crowdfunding.(INSPIER – INSTITUTO DE ENSINO E PESQUISA)

CASTELLS, Manoel. A Galáxia da Internet Reflexões sobre os negócios e a sociedade: Rio de Janeiro, 2003. 7 p. (Jorge Zahar Editor)

GALBRAITH, John Kenneth. Moeda: de onde veio, para onde foi. São Paulo: Pioneira, 1997. 338 p. (Coleção Novos Ubrais).

MILMANN, K. J. and AVAIZIS, M. editors. Scientific Python, volume 11 of Computing in Science & Engineering. IEEE/AIP, March 2011.

MEIRELLES, J. L. F, Júnior T. P, Rebelatto D. P. D, Venture capital e private equity no Brasil: alternativa de financiamento para empresas de base tecnológica 2008

NAKAMOTO, Satoshi(2009)
[http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?](http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A55276)
[commentId=2003008%3AComment%3A55276](http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A55276)

PONTEZA, G.P, Oliveira A, E ,D, Regulando o Growdfunding e o Empreendedorismo no Brasil: Envio | Revista dos Tribunais 25/08/2016

SCHWIENBACHER, A., & Larralde, B. (2012). Alternative types of entrepreneurial finance. In The Oxford Handbook of Entrepreneurial Finance

SZABO, Nick (1996).
[http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html)
[Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html)

ULRICH, Fernando. (2014). Bitcoin: A moeda na era Digital. São Paulo: Instituto Ludwig Von Mises Brasil, 16 p. (1º Edição)

HOWKINS, J. The creative economy: how people make money from ideas. London: Penguin Press, 2001

BEVILÁQUA, Clóvis. Código Civil dos Estados Unidos do Brasil. São Paulo, 1950